**Common Policy CP Change Proposal Number: 2010-06**

| | |
|---|---|
| **To:** | **Federal PKI Policy Authority** |
| **From:** | Certificate Policy Working Group |
| **Subject:** | Proposed modifications to the Common Policy CP |
| **Date:** | September 21, 2010 |
| **Title:** | Allow Federal Legacy PKIs to Directly Cross Certify with Common Policy CA |

**Version and Date of Certificate Policy Requested to be changed:**

X.509 Certificate Policy for the U. S. Federal PKI Common Policy Framework Version 3647 – 1.11, August 16, 2010.

**Change Advocate's Contact Information:**

Name: Judy Spencer
Organization: GSA

**Organization requesting change**: Federal PKI Certificate Policy Working Group

**Change summary**: This change proposal allows Federal Legacy Agencies to directly cross certify with the Common Policy CA.

**Background**: The Common Policy is designed to be the trust anchor for the Federal Government. However, the trust relationship of Federal Legacy PKIs with the Common Policy currently extends through the FBCA. This proposal will allow Federal Legacy PKIs the opportunity to cross-certify with the Common Policy CA if they so desire. By cross-certifying directly with the Common Policy, certificate path construction for the purpose of PIV and internal Federal Government interoperability may be simplified.

Allowing legacy Federal PKIs to cross-certify with the Common Policy will simplify certificate path construction for relying parties that use either Common Policy or the legacy root as the trust anchor in order to validate PIV and other Federal Government credentials.

A policy memo will be issued that informs the Federal Legacy PKIs how their current cross-certification with the FBCA will be transferred to the Common Policy.

**Specific Changes:** Specific changes are made to the following sections: 1.1.4

Insertions are <u>underlined</u>, deletions are in ~~strikethrough~~ text:

### 1.1.4 Interoperation with CAs Issuing under Different Policies

Except for legacy Federal PKIs, ~~Interoperation~~ interoperation with CAs that issue under different policies will be achieved through policy mapping and cross-certification through the Federal Bridge Certification Authority. Legacy Federal PKIs may perform policy mapping and cross-certification with either the Common Policy Root CA or Federal Bridge Certification Authority at their discretion.

Note that interoperability may also be achieved through other means, such as trust lists, to meet local requirements.

**Estimated Cost:**

No additional cost to the Common Policy CA.

**Risk/Impact:**

The risks/impacts of this change primarily affect Federal relying parties that validate credentials from multiple issuers. The legacy Federal PKI should examine its relying party community to determine the ideal method to connect to the Federal PKI (cross-certification with the Common Policy or FBCA). The determination largely depends on the volume of Federally-issued credentials versus externally-issued credentials that need to be validated in addition to the certificate authority that the relying parties use as their trust anchor. Other factors, such as security scenarios, may influence the decision.

- There is no impact on relying parties that only accept locally issued credentials.
- There is no impact on relying parties that rely on trust lists to validate credentials.
- Relying parties that validate Federally-issued credentials (e.g., PIV) against the Common Policy trust anchor should find it simpler to construct paths to legacies that are cross-certified with the Common Policy.
- Relying parties that validate Federally-issued credentials against a legacy trust anchor should find it simpler to construct paths to legacies that are cross-certified with the Common Policy.
- Relying parties that validate externally-issued credentials against the Common Policy trust anchor will experience no change as a result of this change proposal.
- Relying parties that validate externally-issued credentials against a legacy trust anchor may find it simpler to construct paths when the legacy root is cross-certified with the FBCA.

**Implementation Date:**

This change to the policy will be effective immediately upon approval by the FPKIPA and incorporation into the Common Policy CP. Federal Legacy PKIs may change their cross-certification from the FBCA to the Common Policy at their convenience.

**Prerequisites for Adoption:**

The ability to cross-certify with the Common Policy will be limited to Legacy Federal PKIs. The approach to mapping will leverage current mapping with the FBCA and the previous FPKI PA Chair memo regarding the PIV requirements for common-authentication.

**Plan to Meet Prerequisites:**

A memo relating the formal approach to relating the legacy Federal PKI's FBCA mapping to the Common Policy will be issued by the FPKI PA Chair and signed upon approval by the FPKI PA.

**Approval and Coordination Dates:**

Date presented to CPWG: September 21, 2010
Date Presented to FPKIPA TBD
Date of approval by FPKIPA: TBD